

In re Patent Application of:

KURDZIEL

Serial No. **110/792,236**

Filed: **March 03, 2004**

REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application. Attached hereto is one (1) sheet of replacement drawings in which the labeling of Blocks 14 and 22 in FIG. 1 is being corrected.

The independent claims have been amended to include the subject matter from dependent Claims 2, 18 and 30. These dependent claims have been cancelled. The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in amended independent Claim 1, for example, is directed to a block cipher device for a cryptographically secured digital communication system comprising a pair of first stages connected in parallel and receiving an input data block and a control data block. Each first stage defines a respective first data path and comprises a sum modulo-two unit responsive to the control data block and the input data block, and a first nibble swap unit is downstream from the sum modulo-two unit and is responsive to an output signal therefrom and the control data block for reordering the output signal from the sum modulo-two unit.

A diffuser is connected in both of the first data paths for mixing data therebetween. A key scheduler receives a key data block and generates a random key data block based thereon. A pair of second stages is connected in parallel downstream from

In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: March 03, 2004

the first stages and receives the random key data block, the control data block and output signals from the first stages. Each second stage defines a respective second data path and comprises a first linear modulo unit responsive to the random key data block, one of the output signals from the first stages, and the control data block for performing a modulo summing operation based on a first modulus q . An n^{th} power modulo unit is responsive to an output signal from the first linear modulo unit for performing an n^{th} power modulo operation based on a second modulus p . A second linear modulo unit is responsive to the random key data block and an output signal from the n^{th} power modulo unit for performing a modulo summing operation based on a third modulus r . Each first, second and third modulus q , p and r is unique from each other. The pairs of first and second stages are each selectively configurable so that only one first data path and only one second data path are operational while bypassing the diffuser. An output stage is connected to the second stages for generating an output data block for the block cipher device.

The claimed invention advantageously provides a more secure cryptography system that is also compatible with existing less secure cryptography systems. The block cipher device is backward compatible with cryptography systems that are less secure, i.e., those operating with smaller size input data blocks and smaller size key data blocks. Backward compatibility is accomplished by providing the smaller size input data block to only one of the respective first and second data paths in the first and second stages, and by bypassing the bit diffuser.

In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: March 03, 2004

Likewise, the key scheduler may generate a random key data block for the single data path that is operational.

Independent Claim 13 is directed to a communication system comprising the block cipher device for converting an input data block into an output data block, and has been amended similar to independent Claim 1.

Independent Claim 29 is directed to a method for converting an input data block into an output data block for a cryptographically secured digital communication system, and has been amended similar to amended independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 13 and 29 over the Kurdziel et al. patent in view of the Ritter patent. The Examiner cited Kurdziel et al. as disclosing the claimed invention except for a diffuser connected in both of the first data paths for mixing data therebetween. The Examiner cited Ritter as disclosing this feature of the claimed invention.

As best illustrated in FIG. 4 of Kurdziel et al., the illustrated block cipher device 100 includes a first stage for receiving an input data block X and a control data block Z_1 . The first stage defines a first data path, and includes a sum modulo-two unit 1 and a first nibble swap unit 2 downstream from the sum modulo-two unit.

A key scheduler 9 receives a key data block Z_6 and generates a random key data block Z_7 based thereon. A second stage is connected downstream from the first stage and receives the random key data block Z_7 , the control data block Z_5 and output

In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: **March 03, 2004**

signals from the first stage. Each second stage defines a second data path, and includes a first linear modulo unit 5 and an n^{th} power modulo unit 6 downstream from the first linear modulo unit. An output stage 11 is connected to the second stages for generating an output data block for the block cipher device.

As correctly noted by the Examiner, Kurdziel et al. discloses the claimed invention except for the first and second stages being connected in parallel, and a diffuser connected in both of the first data paths for mixing data therebetween. The Examiner cited Ritter as disclosing the diffuser. More particularly, the Examiner referenced FIG. 5a in Ritter as disclosing a pair of first stages 156a, 156b connected in parallel, and a diffuser 152 connected in both of the first data paths for mixing data therebetween.

The Applicants submit that even if the references were selectively combined as suggested by the Examiner, the claimed invention is still not produced. Since Kurdziel et al. discloses first and second stages each with a single data path, Kurdziel et al. obviously fails to teach or suggest this feature of the claimed invention.

Ritter also fails to disclose this feature of the claimed invention. In fact, Ritter teaches away from backward compatibility since cryptography is to be enhanced by using balanced block mixers in combination with other block cipher mechanisms to increase the input block size of the other cipher mechanisms. Cipher mechanisms in Ritter are enhanced by having their block size increased. This increase is achieved using

In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: March 03, 2004

balanced block mixers or arrays of substitution mechanisms to spread an input to the cryptographic mechanism into multiple cipher mechanisms. Cipher mechanisms are also enhanced by transforming their inputs and outputs using balanced block mixers and arrays of substitution mechanisms. Ritter simply fails to teach or suggest any form of backward compatibility with cryptography systems that are less secure, i.e., those operating with smaller size input data blocks and smaller size key data blocks.

In sharp contrast, the claimed invention recites that the pairs of first and second stages are each selectively configurable so that only one first data path and only one second data path are operational while bypassing the diffuser. In the Office Action, the Examiner referenced FIG. 4 and column 2, lines 10-15 in Kurdziel et al. as disclosing "first and second stages being selectively configurable so that one first data path and one second data path are operational." Reference is now directed to column 2, lines 10-15 in Kurdziel et al., which provides:

"The structure of the input unit 10 and output unit 11 generally depends on an application (e.g., serial or parallel)."
(Emphasis added).

It appears that the Examiner has interpreted this to mean that for a "parallel" application, a pair of data paths is used, and that for a "serial" application, only one of the data paths is used. Please note that the Applicant is also an inventor in Kurdziel et al., and the Applicant respectfully

In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: March 03, 2004

submits that the Examiner has erroneously interpreted column 2, lines 10-15 in Kurdziel et al.

The "serial or parallel" application in column 2, lines 10-15 simply refers to whether a host equipment is interfacing the block cipher device 100 via a bus (parallel) or via a serial bit stream. The input and output units 10, 11 format the data coming in from the host equipment into data blocks for processing by the block cipher device 100. For example, if the host equipment provides data via a serial bit stream, the input unit 10 will perform a serial to parallel data conversion. Alternatively, if the data came via a parallel bus, then the input unit 10 would simply accumulate the bus-width packets until a full block was obtained. The same holds true for the output block 11, but only in reverse.

The Examiner appears to have interpreted the above-referenced "serial or parallel" reference as if, depending on the application, you would deploy parallel renderings of the algorithm. This is not correct. The structure of the cryptographic algorithm in Kurdziel et al. conforms to the disclosed theoretical foundation - which operates on a single data path in the first and second stages.

The Applicant recognized the shortfalls of his cited prior art reference, and improved upon it in the present invention while also allowing for backward compatibility with cryptography systems that are less secure, i.e., those operating with smaller size input data blocks and smaller size key data blocks. Backward compatibility is accomplished by providing the

In re Patent Application of:
KURDZIEL
Serial No. 110/792,236
Filed: March 03, 2004

RECEIVED
CENTRAL FAX CENTER
JUN 11 2009

smaller size input data block to one of the respective first and second data paths in the first and second stages, and by bypassing the bit diffuser. Likewise, the key scheduler may generate a random key data block for the single data path that is operational.


Accordingly, it is submitted that amended independent Claim 1 is patentable over Kurdziel et al. in view of Ritter. Amended independent Claims 13 and 29 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Kurdziel et al. in view of Ritter.

In view of the patentability of the amended independent Claims 1, 13 and 29, it is submitted that their dependent claims, which recite yet further distinguishing features of the invention, are also patentable. These dependent claims require no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



In re Patent Application of:

KURDZIEL

Serial No. 110/792,236

Filed: March 03, 2004

MICHAEL W. TAYLOR

Reg. No. 43,182

Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.

255 S. Orange Avenue, Suite 1401

Post Office Box 3791

Orlando, Florida 32802

407-841-2330

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence
has been forwarded via facsimile number 571-273-8300 to the
Commissioner for Patents on this 11 day of June 2009.

Michael W. Taylor
